



# Cisco PIX Security Appliance Release Notes Version 7.2

---

May 2006

## Contents

This document includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Important Notes, page 17](#)
- [Caveats, page 20](#)
- [Obtaining Documentation and Submitting a Service Request, page 28](#)

## Introduction



### Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.2(1).

The Cisco PIX 500 series security appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity through end-point security posture validation and voice and video over VPN support. It also provides enhanced support for intelligent information networks through improved network integration, resiliency, and scalability. This version introduces significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high-availability services, and management/monitoring.

For more information on all the new features, see [New Features, page 4](#)



### Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Additionally, the security appliance software supports ASDM. ASDM is a browser-based, Java applet used to configure and monitor the software on the security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

## System Requirements

The sections that follow list the system requirements for operating a security appliance.



### Note

The PIX 501, PIX 506/506E, and PIX 520 security appliances are not supported in software Version 7.2(1).

## Memory Requirements

If you are using a PIX 515/515E running PIX Version 6.2/6.3, you need to upgrade your memory before performing an upgrade to PIX Version 7.0. PIX Version 7.0 requires at least 64 MB of RAM for Restricted (R) licenses and 128 MB of RAM for Unrestricted (UR) and Failover (FO) licenses. The following security appliance platforms require at least 64 MB of RAM. [Table 1](#) lists Flash memory requirements for Version 7.2(1).

**Table 1** Flash Memory Requirements

Security Appliance Model	Flash Memory Required in Version 7.2(1)
PIX 515/515E	16 MB
PIX 525	16 MB
PIX 535	16 MB

For more information on minimum memory requirements, see “Minimum Memory Requirements” section in the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*.

## Software Requirements

Version 7.2(1) requires the following:

1. The minimum software version required before performing an upgrade to PIX Version 7.2(1) is PIX Version 7.0. If you are running a PIX version prior to PIX Version 6.2, you must first upgrade to PIX Version 6.2 or PIX Version 6.3 before you can begin the upgrade to PIX Version 7.0.

To upgrade your PIX software image, go to the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

2. For information on specific licenses supported on each model of the security appliance, go to the following websites:  
[http://www.cisco.com/en/US/docs/security/asa/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)
3. If you are upgrading from a previous PIX version, save your configuration and write down your activation key and serial number. See <http://www.cisco.com/public/sw-center/index.shtml> for new installation requirements.

## Maximum Recommended Configuration File Size

For the PIX 525 and PIX 535, the maximum supported configuration file size is 2 MB for Version 7.2(1). For the PIX 515/515E, the maximum supported configuration file size is 1 MB for Version 7.2(1). If you are using ASDM, we recommend no more than a 500 KB configuration file because larger configuration files can interfere with the performance of ASDM on your workstation.

While configuration files up to 2 MB are supported on the PIX 525 and PIX 535, be aware that such large configuration files can reduce system performance. For example, a large configuration file is likely to noticeably slow execution times in the following situations:

- While executing commands such as the **write terminal** and **show running-config** commands
- Failover (the configuration synchronization time)
- During a system reload

## Cisco VPN Software Interoperability

Cisco VPN Series	Interoperability Comments
Cisco IOS routers	Version 7.2(1) requires Cisco IOS Release 12.3(T)T or higher running on the router when using IKE Mode Configuration on the security appliance.
Cisco VPN 3000 concentrators	Version 7.2(1) requires Cisco VPN 3000 concentrator Version 3.6 or higher for correct VPN interoperability.

## Cisco VPN Client Interoperability

Cisco VPN Client	Interoperability Comments
Cisco VPN client v3.x/4x (Unified VPN client framework)	Version 7.2(1) supports the Cisco VPN client Version 3.6 or higher that runs on all Microsoft Windows platforms. It also supports the Cisco VPN client Version 3.6 or higher that runs on Linux, Solaris, and Macintosh platforms.

## Cisco Easy VPN Remote Interoperability

Cisco Easy VPN Remote	Interoperability Comments
Cisco PIX Security Appliance Easy VPN remote v6.3	Version 7.2(1) Cisco Easy VPN server requires the Cisco PIX security appliance Version 6.3 Easy VPN remote that runs on the PIX 501 and PIX 506 platforms.

Cisco Easy VPN Remote	Interoperability Comments
VPN 3000 Easy VPN remote v3.x/4x	Version 7.2(1) Cisco Easy VPN server requires the Version 3.6 or higher of the Easy VPN remote that runs on the VPN 3002 platform.
Cisco IOS Easy VPN remote Release 12.2(16.4)T	Version 7.2(1) Cisco Easy VPN server interoperates with Cisco IOS 806 Easy VPN remote Release (16.4)T.

## Determining the Software Version

Use the **show version** command to verify the software version installed on your security appliance.

## Upgrading to a New Software Version

If you have a Cisco.com (CDC) login, you can obtain software from the following website:

<http://www.cisco.com/public/sw-center/index.shtml>

If you want to upgrade or downgrade from Version 7.0.(x) to 7.1(x) and vice versa You must follow the steps below because older versions of the security appliance images does not recognize new ASDM images, new security appliance images does not recognize old ASDM images.

To upgrade from Version 7.1.(x) to 7.2(x), you must perform the following steps:

- 
- Step 1** Load the new Version 7.2(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 2** Reload the device so that it will start using the Version 7.2(x) image.
- Step 3** Copy new ASDM Version 5.2(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- 

To downgrade from Version 7.2(x) to 7.1.(x), you must perform the following steps:

- 
- Step 1** Load the earlier Version 7.1(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 2** Reload the device so that it will be use the Version 7.1(x) image.
- Step 3** Copy the ASDM Version 5.1(x) image from the following website:  
<http://www.cisco.com/public/sw-center/index.shtml>
- 

## New Features

This section describes the new features in this version. This section includes the following topics:

- [Application Inspection and Control, page 5](#)

- [Remote Access and Site-to-Site VPN, page 9](#)
- [Network Integration, page 12](#)
- [Resiliency and Scalability, page 13](#)
- [Other Enhancements, page 14](#)
- [Management and Serviceability, page 16](#)

## Application Inspection and Control

This section includes the following topics:

- [Enhanced ESMTP Inspection, page 5](#)
- [DCERPC Inspection, page 5](#)
- [Enhanced NetBIOS Inspection, page 6](#)
- [Enhanced H.323 Inspection, page 6](#)
- [Enhanced DNS Inspection, page 6](#)
- [Enhanced FTP Inspection, page 6](#)
- [Enhanced HTTP Inspection, page 7](#)
- [Enhanced Skinny \(SCCP\) Inspection, page 7](#)
- [Enhanced SIP Inspection, page 7](#)
- [Instant Messaging \(IM\) Inspection, page 8](#)
- [MPF-Based Regular Expression Classification Map, page 8](#)
- [Radius Accounting Inspection, page 8](#)
- [GKRCS Support for H.323, page 8](#)
- [Skinny Video Support, page 8](#)
- [SIP IP Address Privacy, page 9](#)

### Enhanced ESMTP Inspection

This feature allows you to detect attacks, including spam, phishing, malformed message attacks, and buffer overflow and underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detects several attacks, blocks senders and receivers, and blocks mail relay.

For more information, see the “ESMTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### DCERPC Inspection

This feature allows you to change the default configuration values used for DCERPC application inspection using a DCERPC inspect map.

DCERPC is a protocol used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

Typically, a client queries a server called the Endpoint Mapper (EPM) that listens on a well-known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance that provides the service. The security appliance allows the appropriate port number and network address and also applies NAT or PAT, if needed, for the secondary connection.

For more information, see the “DCERPC Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced NetBIOS Inspection

This feature allows you to change the default configuration values used for NetBIOS application inspection.

NetBIOS application inspection performs NAT for the embedded IP address in the NetBIOS name service packets and NetBIOS datagram services packets. It also enforces protocol conformance by checking the various count and length fields for consistency.

For more information, see the “NetBIOS Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced H.323 Inspection

This feature allows you to change the default configuration values used for H.323 application inspection.

H.323 inspection supports RAS, H.225, and H.245, and its functionality translates all embedded IP addresses and ports. It performs state tracking and filtering and can do a cascade of inspect function activation. H.323 inspection supports phone number filtering, dynamic T.120 control, H.245 tunneling control, protocol state tracking, H.323 call duration enforcement, and audio and video control.

For more information, see the “H.323 Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced DNS Inspection

This feature allows you to specify actions when a message violates a parameter that uses a DNS inspection policy map. DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow filtering based on the DNS header, domain name, and resource record TYPE and CLASS.

For more information, see the “DNS Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced FTP Inspection

This feature allows you to change the default configuration values used for FTP application inspection.

FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation.

Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.

For more information, see the “FTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced HTTP Inspection

This feature allows you to change the default configuration values used for HTTP application inspection.

HTTP application inspection scans HTTP headers and body and performs various checks on the data. These checks prevent various HTTP constructs, content types, and tunneling and messaging protocols from traversing the security appliance.

HTTP application inspection can block tunneled applications and non-ASCII characters in HTTP requests and responses, preventing malicious content from reaching the web server. Size limiting of various elements in HTTP request and response headers, URL blocking, and HTTP server header type spoofing are also supported.

For more information, see the “HTTP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced Skinny (SCCP) Inspection

This feature allows you to change the default configuration values used for SCCP (Skinny) application inspection.

Skinny application inspection performs translation of embedded IP address and port numbers within the packet data and dynamic opening of pinholes. It also performs additional protocol conformance checks and basic state tracking.

For more information, see the “Skinny (SCCP) Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Enhanced SIP Inspection

This feature allows you to change the default configuration values used for SIP application inspection.

SIP is a widely used protocol for Internet conferencing, telephony, events notification, and instant messaging. Partially because of its text-based nature and partially because of its flexibility, SIP networks are subject to a large number of security threats.

SIP application inspection provides address translation in the message header and body, dynamic opening of ports, and basic sanity checks. It also supports application security and protocol conformance, which enforces the sanity of the SIP messages, as well as detects SIP-based attacks.

For more information, see the “SIP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Instant Messaging (IM) Inspection

This feature allows you to change the default configuration values used for Instant Messaging (IM) application inspection.

Instant Messaging (IM) application inspection provides detailed access control to control network usage. It also helps stop leakage of confidential data and propagations of network threats. A regular expression database search that represents various patterns for Instant Messaging (IM) protocols to be filtered is applied. A syslog is generated if the flow is not recognized.

The scope can be limited by using an access list to specify any traffic streams to be inspected. For UDP messages, a corresponding UDP port number is also configurable. Inspection of Yahoo! Messenger and MSN Messenger instant messages are supported.

For more information, see the “Instant Messaging Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## MPF-Based Regular Expression Classification Map

This feature allows you to define regular expressions in Modular Policy Framework class maps and match a group of regular expressions that has the **match-any** attribute. You can use a regular expression class map to match the content of certain traffic; for example, you can match URL strings inside HTTP packets.

For more information, see the “Creating a Regular Expression Class Map” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Radius Accounting Inspection

This feature allows you to protect against an over-billing attack in the Mobile Billing Infrastructure. The **policy-map type inspect radius-accounting** command was introduced in this version.

For more information, see the “Configuring Application Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## GKRCS Support for H.323

Two control signaling methods are described in the ITU-T H.323 recommendation: Gatekeeper Routed Control Signaling (GKRCS) and Direct Call Signalling (DCS). DCS is supported by the Cisco IOS gatekeeper. This feature adds Gatekeeper Routed Control Signaling (GKRCS) control signaling method support.

For more information, see the “H.323 Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Skinny Video Support

This feature adds SCCP version 4.1.2 message support to print the message name processed by the inspect feature when **debug skinny** is enabled. CCM 4.0.1 messages are supported.



For more information, see the “Skinny (SCCP) Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## SIP IP Address Privacy

This feature allows you to retain the outside IP addresses embedded in inbound SIP packets for all transactions, except REGISTER (because it is exchanged between the proxy and the phone), to hide the real IP address of the phone. The REGISTER message and the response to REGISTER message will be exempt from this operation because this message is exchanged between the phone and the proxy.

When this feature is enabled, the outside IP addresses in the SIP header and SDP data of inbound SIP packets will be retained. Use the **ip-address-privacy** command to turn on this feature.

For more information, see the “SIP Inspection” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Remote Access and Site-to-Site VPN

This section includes the following topics:

- [Network Admission Control, page 9](#)
- [L2TP Over IPsec, page 10](#)
- [OCSP Support, page 10](#)
- [Active RIP Support, page 11](#)
- [Multiple L2TP Over IPsec Clients Behind NAT, page 11](#)
- [Nokia Mobile Authentication Support, page 11](#)
- [Zonelabs Integrity Server, page 11](#)
- [Hybrid XAUTH, page 11](#)
- [IPsec Fragmentation and Reassembly Statistics, page 12](#)

## Network Admission Control

Network Admission Control (NAC) allows you to validate a peer based on its state. This method is referred to as posture validation (PV). PV can include verifying that the peer is running applications with the latest patches, and ensuring that the antivirus files, personal firewall rules, or intrusion protection software that runs on the remote host are up to date.

An Access Control Server (ACS) must be configured for Network Admission Control before you configure NAC on the security appliance.

As a NAC authenticator, the security appliance does the following:

- Initiates the initial exchange of credentials based on IPsec session establishment and periodic exchanges thereafter.
- Relays credential requests and responses between the peer and the ACS.
- Enforces the network access policy for an IPsec session based on results from the ACS server.
- Supports a local exception list based on the peer operating system, and optionally, an ACL.

- (Optional) Requests access policies from the ACS server for a clientless host.

As an ACS client, the security appliance supports the following:

- EAP/RADIUS
- RADIUS attributes required for NAC

NAC on the security appliance differs from NAC on Cisco IOS Layer 3 devices (such as routers) where routers trigger PV based on routed traffic. The security appliance enabled with NAC uses an IPsec VPN session as the trigger for PV. Cisco IOS routers configured with NAC use an Intercept ACL to trigger PV based on traffic destined for certain networks. Because external devices cannot access the network behind the security appliance without starting a VPN session, the security appliance does not need an intercept ACL as a PV trigger. During PV, all IPsec traffic from the peer is subject to the default ACL configured for the peer's group.

Unlike the Cisco VPN 3000 Concentrator Series, NAC on the security appliance supports stateless failover, initialization of all NAC sessions in a tunnel group, revalidation of all NAC sessions in a tunnel group, and posture validation exemption lists configured for each tunnel group. NAC on the security appliance does not support non-VPN traffic, IPv6, security contexts, and WebVPN.

By default, NAC is disabled. You can enable it on a group policy basis.

For more information, see the “Configuring Network Admission Control” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## L2TP Over IPsec

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to communicate securely with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data. L2TP is based on the client/server model. The function is divided between the L2TP Network Server (LNS), and the L2TP Access Concentrator (LAC). The LNS typically runs on a network gateway such as a router, while the LAC can be a dial-up Network Access Server (NAS), or a PC with a bundled L2TP client such as Microsoft Windows 2000.

L2TP/IPsec provides the capability to deploy and administer an L2TP VPN solution alongside the IPsec VPN and firewall services in a single platform.

The primary benefit of configuring L2TP with IPsec in a remote access scenario is that remote users can access a VPN over a public IP network without a gateway or a dedicated line, enabling remote access from virtually anyplace with POTS. An additional benefit is that the only client requirement for VPN access is the use of Windows 2000 with Microsoft Dial-Up Networking (DUN). No additional client software, such as Cisco VPN client software, is required.

For more information, see the “Configuring L2TP over IPsec” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## OCSP Support

The Online Certificate Status Protocol (OCSP) provides an alternative to CRL for obtaining the revocation status of X.509 digital certificates. Rather than requiring a client to download a complete and often large certificate revocation list, OCSP localizes the certificate status on a Validation Authority, which it queries for the status of a specific certificate.

## Active RIP Support

The security appliance supports RIP Version 1 and RIP Version 2. You can only enable one RIP routing process on the security appliance. When you enable the RIP routing process, RIP is enabled on all interfaces. By default, the security appliance sends RIP Version 1 updates and accepts RIP Version 1 and Version 2 updates.

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode.

For more information, see the “Configuring RIP” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Multiple L2TP Over IPsec Clients Behind NAT

The security appliance can successfully establish remote-access L2TP-over-IPsec connections to more than one client behind one or more NAT devices. This enhances the reliability of L2TP over IPsec connections in typical SOHO/branch office environment environments, where multiple L2TP over IPsec clients must communicate securely with a central office.

For more information, see the “Configuring L2TP over IPSec” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Nokia Mobile Authentication Support

You can establish a VPN using a handheld Nokia 92xx Communicator series cellular device for remote access. The authentication protocol that these devices use is the IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) protocol.

For more information, see the “Supporting the Nokia VPN Client” section in the *Cisco Security Appliance Command Line Configuration Guide*.

## Zonelabs Integrity Server

You can configure the security appliance in a network that deploys the Zone Labs Integrity System to enforce security policies on remote VPN clients. In this case, the security appliance is an edge gateway between the Zone Labs Integrity server and the remote clients. The Zone Labs Integrity server and the Zone Labs Personal Firewall on the remote client ensure that a remote client complies with a centrally managed security policy before the client can access private network resources. You configure the security appliance to pass security policy information between the server and clients to maintain or close client connections to prevent a server connection failure, and to optionally, require SSL certificate authentication of both the Integrity server and the security appliance.

For more information, see the “Configuring Integrity Server Support” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Hybrid XAUTH

You can configure hybrid authentication to enhance the IKE security between the security appliance and remote users. With this feature, IKE Phase I requires two steps. The security appliance first authenticates to the remote VPN user with standard public key techniques and establishes an IKE security association

that is unidirectionally authenticated. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use any one of the supported authentication methods. Hybrid XAUTH allows you to use digital certificates for security appliance authentication and a different method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID.

## IPsec Fragmentation and Reassembly Statistics

You can monitor additional IPsec fragmentation and reassembly statistics that help to debug IPsec-related fragmentation and reassembly issues. The new statistics provide information about fragmentation and reassembly both before and after IPsec processing.

## Network Integration

This section includes the following topics:

- [PPPoE Client, page 12](#)
- [Dynamic DNS Support, page 12](#)
- [Multicast Routing Enhancements, page 13](#)
- [Private and Automatic MAC Address Assignments and Generation for Multiple Context Mode, page 13](#)
- [Expanded DNS Domain Name Usage, page 13](#)

## PPPoE Client

Point-to-Point Protocol over Ethernet (PPPoE) combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. PPPoE clients are typically personal computers connected to an ISP over a remote broadband connection, such as DSL or cable service. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.

For more information, see the “Configuring the PPPoE Client” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Dynamic DNS Support

You can create dynamic DNS (DDNS) update methods and configure them to update the Resource Records (RRs) on the DNS server at whatever frequency you need.

DDNS complements DHCP, which enables users to dynamically and transparently assign reusable IP addresses to clients. DDNS then provides dynamic updating and synchronizing of the name to the address and the address to the name mappings on the DNS server. With this version, the security appliance supports the IETF standard for DNS record updates.

For more information, see the “Configuring DHCP and DDNS Services” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Multicast Routing Enhancements

Multicast routing enhancements allows you to define multicast boundaries so that domains with RPs that have the same IP address do not leak into each other, to filter PIM neighbors to better control the PIM process, and to filter PIM bidir neighbors to support mixed bidirectional and sparse-mode networks.

For more information, see the “Configuring Multicast Routing” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

## Private and Automatic MAC Address Assignments and Generation for Multiple Context Mode

You can assign a private MAC address (both active and standby for failover) for each interface. For multiple context mode, you can automatically generate unique MAC addresses for shared context interfaces, which makes classifying packets into contexts more reliable.

The new **mac-address auto** command allows you to automatically assign private MAC addresses to each shared context interface.

For more information, see the “Automatically Assigning MAC Addresses to Context Interfaces” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Expanded DNS Domain Name Usage

You can use DNS domain names, such as `www.example.com`, when configuring AAA servers and also with the **ping**, **tracert**, and **copy** commands.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Resiliency and Scalability

This section includes the following topics:

- [Sub-second Failover, page 13](#)
- [Standby ISP Support, page 13](#)

### Sub-second Failover

This feature allows you to configure failover to detect and respond to failures in under a second.

For more information, see the “Configuring Failover” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

### Standby ISP Support

This feature allows you to configure a link standby ISP if the link to your primary ISP fails. It uses static routing and object tracking to determine the availability of the primary route and to activate the secondary route when the primary route fails.

For more information, see the “Configuring IP Routing and DHCP Services” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

## Other Enhancements

This section includes the following topics:

- [RTP/RTCP Inspection, page 14](#)
- [Generic Input Rate Limiting, page 14](#)
- [URL Filtering Enhancements for Secure Computing \(N2H2\), page 14](#)
- [Resource Management for Security Contexts, page 15](#)
- [Authentication for Through Traffic and Management Access Supports All Servers Previously Supported for VPN Clients, page 15](#)
- [Auto Update, page 15](#)
- [Dead Connection Detection \(DCD\), page 15](#)
- [Configurable Prompt, page 15](#)
- [Save All Context Configurations from the System, page 16](#)
- [Intra-Interface Communication for Clear Traffic, page 16](#)
- [Modular Policy Framework Support for Management Traffic, page 16](#)

### RTP/RTCP Inspection

This feature NATs embedded IP addresses and opens pinholes for RTP and RTCP traffic. This feature ensures that only RTP packets flow on the pinholes opened by Inspects SIP, Skinny, and H.323. To prevent a malicious application from sending UDP traffic to make use of the pinholes created on the security appliance, this feature allows you to monitor RTP and RTCP traffic and to enforce the validity of RTP and RTCP packets.

For more information, see the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### Generic Input Rate Limiting

This feature prevents denial of service (DoS) attacks on a security appliance or on certain inspection engines on a firewall. The 7.0 release supports egress rate-limiting (police) functionality and in this release, input rate-limiting functionality extends the current egress policing functionality.

The **police** command is extended for this functionality.

For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### URL Filtering Enhancements for Secure Computing (N2H2)

This feature allows you to enable long URL, HTTPS, and FTP filtering by using both Websense (the current vendor) and N2H2 (a vendor that has been purchased by Secure Computing). Previously, the code only enabled the vendor Websense to provide this type of filtering. The url-block, url-server, and filter commands provide support for this feature.

For more information, see the “Applying Filtering Services” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Resource Management for Security Contexts

If you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

For more information, see the “Configuring Resource Management” section in the *Cisco Security Appliance Command Line Configuration Guide*.

## Authentication for Through Traffic and Management Access Supports All Servers Previously Supported for VPN Clients

All server types can be used for firewall authentication with the following exceptions: HTTP Form protocol supports single sign-on authentication for WebVPN users only and SDI is not supported for HTTP administrative access.

For more information, see the “Summary of Support” section in the *Cisco Security Appliance Command Line Configuration Guide*.

## Auto Update

The security appliance can now be configured as an Auto Update server in addition to being configured as an Auto Update client. The existing **client-update** command (which is also used to update VPN clients) is enhanced to support the new Auto Update server functionality, and includes new keywords and arguments that the security appliance needs to update security appliances configured as clients. For the security appliance configured as an Auto Update client, the auto-update command continues to be the command used to configure the parameters that the security appliance needs to communicate with the Auto Update server.

For more information, see the “Configuring Auto Update Support” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Dead Connection Detection (DCD)

This feature allows the security appliance to automatically detect and expire dead connections. In previous versions, dead connections never timed out; they were given an infinite timeout. Manual intervention was required to ensure that the number of dead connections did not overwhelm the security appliance. With this feature, dead connections are detected and expired automatically, without interfering with connections that can still handle traffic. The **set connection timeout** and **show service-policy** commands provide DCD support.

For more information, see the “Configuring Connection Limits and Timeouts” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Configurable Prompt

With this feature, the user can see the failover status of the security appliance without having to enter the **show failover** command and parse the output. This feature allows users to see the chassis slot number of the failover unit. Previously, the prompt reflected just the hostname, security context, and configuration mode. The **prompt** command provides support for this feature.

For more information, see the “Using the Command Line Interface” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Save All Context Configurations from the System

You can now save all context configurations at once from the system execution space using the **write memory all** command.

For more information, see the “Device Initialization and Configuration Synchronization” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## Intra-Interface Communication for Clear Traffic

You can now allow any traffic to enter and exit the same interface, and not just VPN traffic. For more information, see the “Permitting Intra-Interface Traffic” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

## Modular Policy Framework Support for Management Traffic

You can now define a Layer 3/4 class map for to-the-security-appliance traffic, so you can perform special actions on management traffic. For this version, you can inspect RADIUS accounting traffic.

For more information, see the “Using the Modular Policy Framework” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

## Management and Serviceability

This section includes the following topics:

- [Traceroute, page 16](#)
- [Packet Tracer, page 16](#)
- [WCCP, page 17](#)
- [IPv6 Security Enforcement of IPv6 Addresses, page 17](#)
- [Inspection IPS, CSC and URL Filtering for WebVPN, page 17](#)

### Traceroute

The traceroute command allows you to trace the route of a packet to its destination.

For more information, see the “Traceroute” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

### Packet Tracer

The packet tracer tool allows you to trace the life span of a packet through the security appliance to see if it is behaving as expected.



The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. If a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause.

For more information, see the “Packet Tracer” section in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

## WCCP

The Web Cache Communication Protocol (WCCP) feature allows you to specify WCCP service groups and redirect web cache traffic. The feature transparently redirects selected types of traffic to a group of web cache engines to optimize resource usage and lower response times.

## IPv6 Security Enforcement of IPv6 Addresses

This feature allows you to configure the security appliance to require that IPv6 addresses for directly connected hosts use the Modified EUI-64 format for the interface identifier portion of the address.

For more information, see the “Configuring IPv6” chapter in the *Cisco Security Appliance Command Line Configuration Guide*.

## Inspection IPS, CSC and URL Filtering for WebVPN

This feature adds support for inspection, IPS, and Trend Micro for WebVPN traffic in clientless mode and port forwarding mode. Support for SVC mode is preexisting. In all of the modes, the Trend Micro and the IPS engines will be triggered (if configured).

URL/FTP/HTTPS/Java/Activex filtering using WebSense and N2H2 support has also been added. DNS inspect will be triggered for the DNS requests.

In port forwarding mode, HTTP, SMTP, FTP, and DNS inspections with the filtering mechanisms using WebSense and N2H2 support has been added.

For more information, see the “Configuring WebVPN” chapter in the *Cisco Security Appliance Command Line Configuration Guide*. For a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

# Important Notes

This section lists important notes related to Version 7.2(1).

## HTTP(S) Authentication Challenge Improvement

In versions prior to 7.2(1), the security appliance authenticated HTTP network connections using basic HTTP authentication and authenticated HTTPS connections by generating similar custom login windows. In 7.2(1), HTTP and HTTPS connections are redirected to a set of authentication pages that are served directly by the security appliance. After successful authentication, the browser is again redirected to the originally-intended URL. When AAA is configured, these pages are available at:

[http://interface\\_ip:1080/netaccess/connstatus.html](http://interface_ip:1080/netaccess/connstatus.html)

[https://interface\\_ip:1443/netaccess/connstatus.html](https://interface_ip:1443/netaccess/connstatus.html)

## FIPS 140-2

The security appliance Version 7.0(4) is FIPS certified. Version 7.1 is on the FIPS 140-2 Pre-Validation List.

## Maximum Security Contexts and VLANs Supported

The maximum security contexts supported in Version 7.2(1) for the PIX 535 are 50 tiers. The maximum number of VLANs supported are 150. For more information on the feature support for each platform license, see the “Platform Feature Licenses” section in the *Cisco Security Appliance Command Line Configuration Guide*.

## IKE Delete-with-Reason

IKE syslogs for Delete-with-Reason do not contain the reason text unless the clients support this feature. Currently, the VPN 3002 Version 4.7 and PIX 501 Version 6.3(4) hardware clients do not support this feature.

**Note**

The PIX 501 security appliance is not supported in software Version 7.2(1).

## User Upgrade Guide

Before upgrading to Version 7.2(1), read the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading in Cisco PIX Software Version 7.0*. This guide includes information about deprecated features and other changes in the Cisco PIX Software Version 7.0. For a list of deprecated features and user upgrade information, go to the following URL:

[http://www.cisco.com/en/US/docs/security/asa/asa70/pix\\_upgrade/upgrade/guide/pixupgrd.html](http://www.cisco.com/en/US/docs/security/asa/asa70/pix_upgrade/upgrade/guide/pixupgrd.html)

**Caution**

If you share the Stateful Failover update link with a link for regular traffic such as your inside interface, you must change your configuration before upgrading. Do not upgrade until you have corrected your configuration, as this is not a supported configuration and Version 7.2(1) treats the LAN failover and Stateful Failover update interfaces as special interfaces. If you upgrade to Version 7.2(1) with a configuration that shares an interface for both regular traffic and the Stateful Failover updates, configuration related to the regular traffic interface will be lost after the upgrade. The lost configuration may prevent you from connecting to the security appliance over the network.

## Readme Document for the Conduits and Outbound List Conversion Tool 1.2

The security appliance Outbound and Conduit Conversion tool assists in converting configurations with **outbound** or **conduit** commands to similar configurations using ACLs. ACL-based configurations provide uniformity and optimize the ACL feature set. ACL-based configurations provide the following benefits:

- ACE insertion capability — Provides simplified system configuration and management, which allows you to add, delete or modify individual ACEs.
- Outbound ACLs and time-based ACLs— Provides administrators with improved flexibility for defining access control policies by adding support for outbound ACLs and time-based ACLs.
- Enabling and Disabling of ACL entries — Provides a convenient troubleshooting tool that allows administrators to test and fine-tune ACLs without the need to remove and replace ACL entries.

## MIBs Support

The Cisco Unified Firewall MIB offers a unified SNMP standards-based monitoring interface for functionality on the security appliances. The Unified Firewall MIB offers statistics collection and monitoring for Stateful Packet Inspection, URL Filtering, and Application Inspection.

For more information on MIB Support, go to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## Features not Supported in Version 7.2(1)

The PPTP feature is not supported in Version 7.2(1).

## Downgrade to Previous Version

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.

For more information and a complete description of the command syntax, see the *Cisco Security Appliance Command Reference*.

**Caution**

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. If you load a software image from monitor mode onto a PIX security appliance that has a PIX Version 7.0 file system, unpredictable behavior may occur and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

## Caveats

The following sections describe the caveats for the Version 7.2(1).

For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

## Open Caveats - Version 7.2(1)

**Table 2**      **Open Caveats**

DDTS Number	Software Version 7.2(1)	
	Corrected	Caveat
CSCse37315	No	AIC DNS - Traceback after removing certain MPF actions with DNS traffic
CSCse38087	No	RFW:multi-mode kerberos authentication fails after few hours stress test
CSCse28871	No	NAC: Session entries are not cleaned up after initial posture validation
CSCse28930	No	NAC: Posture validation failure due to inconsistent source IP address
CSCse24058	No	L2TP: Traffic denied through tunnel after 2 days -> domain=aaa-user
CSCse22760	No	LDAP/Sun, Pass expires in X days is not functioning properly
CSCse34477	No	ESMTP: mail-relay param w/o any action accepted, junk chars in sho run
CSCse34515	No	ESMTP: mail-relay action drop-connection log taken as drop-connection

**Table 2**      **Open Caveats**

DDTS Number	Software Version 7.2(1)	
CSCse29150	No	ESMTP: match not conditions related to count not working
CSCse20854	No	ESMTP: multiple match cond. with regex - only most generic regex matched
CSCse38371	No	IM: MSN drop-connection not enforced is specific scenarios
CSCse32684	No	IM: match not version does not block for Yhoo IM
CSCse27787	No	AIC SIP: SIP messages might fail state-check knob when record-route on
CSCse20834	No	SIP: BYE embryonic connection timestamp not updated for re-Invite
CSCse37065	No	Proxy erroneously drops ACK bit in RST causing Kerberos rsh to fail
CSCse27774	No	PPPoE Object-tracking: Traceback in IP Thread when disabling pppoe
CSCsd84011	No	REGEX: ^ (match from beginning of text) does not work in some cases
CSCsd82575	No	unexpected IGMP joins sent when configuring multicast routing
CSCsd59295	No	WCCP static bypass not working with vlan interfaces
CSCsd51407	No	Dual ISP fails after failover, routing table have stale routes
CSCse32481	No	errmsg:xfer_encode regex missing for 1st xfer_encode count command
CSCse32774	No	Cisco MacOS VPN client disconnects after rekey.
CSCse29692	No	L2TP: File transfers with any client in my setup results in tunnel drop
CSCse29635	No	L2TP/IPSec: sporadic tunnel drops occur after numerous rekeys
CSCse21175	No	IPSec RAS performance on ASA-5540 is down approx 11% versus 7.1.2
CSCse21150	No	L2TP: Mac client dropping sessions during overnight system test
CSCse09534	No	L2TP: windows file transfer of large files sometimes fails
CSCsd78808	No	L2TP: Fragmentation reassembly issues with PIX VAC and L2TP conns
CSCsd45605	No	2 routes to same n/w w same metric different ifx should not be allowed
CSCse24537	No	RIP: [no] access-list defined in distribute-list should display err msg
CSCse31519	No	OCSF: CRL checking of externally signed responder cert fails
CSCse33851	No	H.225 releasecomplete message was dropped by the firewall
CSCse39315	No	t120 fax cannot get through multiple routed mode
CSCse39263	No	h.323 packet drop when connecting in multiple mode

## Resolved Caveats - Version 7.2(1)

**Table 3**      **Resolved Caveats**

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCdy45820	Yes	show traffic broken, add 5 mins traffic info to show interface
CSCee29967	Yes	MFW: system context cannot log to external syslog server

**Table 3** *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCeh01744	Yes	Undo CSCdy82442 and support 10 dhcprelay statements on FWSM
CSCeh59278	Yes	DHCPACK gets dropped when it is sent in response to DHCPINFORM
CSCeh60845	Yes	Logginig queue incorrectly registers 8192 256-byte blocks
CSCeh70043	Yes	DOC: sh asp drop needs further clarification in doc
CSCeh90617	Yes	Recompiling ACLs can cause packet drops on low-end platforms
CSCei43588	Yes	traceback when trying to match a packet to acl with deny
CSCei47678	Yes	SNMP packet size standards in RFC3417 not fully supported.
CSCek21835	Yes	Higher metric OSPF external route is selected
CSCek21836	Yes	SIP: BYE embryonic connection timestamp not updated.
CSCek21837	Yes	PDM with Command Authorization requires the write command for Read-Only
CSCek21838	Yes	SIP: fail to open a conn for Record route in NOTIFY
CSCek21843	Yes	SIP: Not translate c= address if first m= has port 0 in SDP body.
CSCek21846	Yes	SIP: xlate timeout not updated by Expire value in Register message
CSCek21849	Yes	Backspace sent in cut-through proxy authentication
CSCek26572	Yes	tftp fixup does not allow error message from client
CSCek40279	Yes	Increase in CPU utilization when OSPF is enabled
CSCsb80170	Yes	VPN3K PARITY: Address-pools needed in group-policy
CSCsb94408	Yes	FWSM Thread dhcp_daemon crashing randomly
CSCsc12094	Yes	AAA fallback authentication does not work with reactivation-mode timed
CSCsc15434	Yes	Assertion violation w/icmp traffic and icmp inspection
CSCsc16041	Yes	'clear local host' results in memory leak
CSCsc16507	Yes	Cannot remove url-server despite having removed url-block cmd
CSCsc18324	Yes	Traceback in Dispatch Unit (Old pc 0x001dbdc6 ebp 0x01212404)
CSCsc18911	Yes	PIX / ASA does not remove OSPF route for global PAT entry after deleting
CSCsc29201	Yes	ASA Management 0/0 interface cannot be used in Transparent mode for OOB
CSCsc33385	Yes	GTP - pdp context creation failed - GSN tunnel limit exceeded
CSCsc39334	Yes	Traceback due to check-retransmission from the tcp-map
CSCsc44591	Yes	Traceback in Thread Name: ARP Thread in multicontext mode
CSCsc46976	Yes	SIP: traceback when failed to pre-allocate early rtp
CSCsc47618	Yes	Authenticate all messages between Active and Standby Firewalls
CSCsc51737	Yes	AIC SIP: Add support for m=text
CSCsc51939	Yes	Performance throughput problems when http inspect enabled
CSCsc68575	Yes	CPU usage is higher for given traffic throughput in recent releases.
CSCsc73942	Yes	TCP RST is dropped when there is outstanding data that is not acked
CSCsc78900	Yes	Reload with Thread Name: Dispatch Unit at tcp_check_packet

**Table 3**     *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCsc79110	Yes	syslogs show user <unknown> when packets denied by vpn-filter
CSCsc81565	Yes	Idle conn timeout reset when packet dropped by TCP normalizer
CSCsc81668	Yes	<a href="https://&lt;ip&gt;/config">https://&lt;ip&gt;/config</a> does not have the same privilege level as 'write'
CSCsc83471	Yes	incorrect IPSec SA's may be deleted upon receiving DELETE notify
CSCsc86217	Yes	Voice Proxy Function does not preserve DSCP bits.
CSCsc90826	Yes	PIX 7.0 getting the error %PIX-1-106021 when ip verify command enable
CSCsc90944	Yes	Malformed https proxy authentication page w/ linebreak
CSCsc91450	Yes	FTP control channel timing out although data channel is active.
CSCsc92575	Yes	Upgrade Activation Key reduces permitted interfaces
CSCsc93061	Yes	Traceback after activation of vpn-filter
CSCsc94945	Yes	Startup-config error with priority-queue and service-policy
CSCsc97846	Yes	Significant CPU utilization increase when adding more logging hosts.
CSCsc97999	Yes	Syslog Message ID 313003 is used incorrectly
CSCsc98339	Yes	Standby unit may reload if active unit powered off
CSCsc99263	Yes	GTPv1: Subsequent Create Req to modify PDP context IEs are not processed
CSCsc99364	Yes	SSL Certs from Verisign Managed PKI do not install
CSCsd00051	Yes	SNMP polling of ASA management interface stats may cause packet loss
CSCsd00175	Yes	ASA w/ IPS may drop FIN/ACK packets resulting in half open FTP sessions
CSCsd01722	Yes	PIX/ASA 7.0 logging message 419001 always sent in message lists
CSCsd02938	Yes	ASA/PIX doesn't reconnect if websense server goes down
CSCsd03391	Yes	TCP Intercept doesn't negate CPU impact when SYN flood from adjacent net
CSCsd03664	Yes	Reload w/ Thread Name:Session Manager w/ high volume of L2L VPN traffic
CSCsd04327	Yes	ASA out of order packets to ssm or inspect are dropped
CSCsd04700	Yes	match port option for setting connection time-outs does not work
CSCsd07703	Yes	Oracle Forms(Java) Applet not loading via WebVPN
CSCsd07783	Yes	Transient NAT-T packets silently dropped if NAT-T is enabled
CSCsd08170	Yes	UDP 500 not removed from pat port pool when crypto map is applied
CSCsd10138	Yes	Traceback in Checkheaps thread when enabling LAN2LAN vpn
CSCsd11179	Yes	SNMP polling of resource MIBS may cause packet loss
CSCsd11511	Yes	Traceback due to memory corruption in sanity check of Checkheaps thread
CSCsd12670	Yes	ASA, WebVPN errors when triggering a simple javascript
CSCsd13334	Yes	Memory Leaking tunnel-group authorization-dn-attributes
CSCsd13636	Yes	Reload with thread name dispatch unit
CSCsd15475	Yes	Secondary unit doesn't get full config file after SSH reload on Primary
CSCsd16751	Yes	GTP: wrong service-policy used when connection is re-used

**Table 3** *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCsd16780	Yes	Assertion in indirect->timestamp & pool->timestamp_mask) == timestamp
CSCsd17182	Yes	no nat-control does not appear in the output of show run all
CSCsd17431	Yes	Managment rule addition / tracking needs to be cleaned up
CSCsd17598	Yes	svc image <imagename> fails to set svc image after clear conf all
CSCsd17718	Yes	IGMP forward interface command fails to sync to the standby unit
CSCsd17763	Yes	Firewall should not respond to TCP segment w/ RST+ACK and bad ACK number
CSCsd17879	Yes	Deny rules in crypto acl blocks inbound tcp/udp after tunnel formed
CSCsd21887	Yes	WebVPN mangles the url's in emails when accessing OWA
CSCsd22910	Yes	users with passwords longer than 11 chars can no longer authenticate
CSCsd25537	Yes	Failover unit traceback in Thread Name: fover_FSM_thread
CSCsd25553	Yes	Traceback when VPN client tries to make connection to inside interface
CSCsd25975	Yes	Add file URL support to WebVPN clientless mode
CSCsd28581	Yes	Failover: Standby device may traceback in Thread Name: IKE Daemon
CSCsd30371	Yes	Show vpnsession-db remote displays incorrect group-policy
CSCsd31334	Yes	Need a way to clear a subset of arps
CSCsd33677	Yes	ssl handshake failure occurs for SVC clients when re-keing using SSL
CSCsd34070	Yes	H.245 inspect skipped if GK RCS and wrong H.225 callSignalAddress for GK
CSCsd36030	Yes	in multiple policy-maps, packets should match the first map, not the last
CSCsd37075	Yes	PIX/ASA reload in Thread Name PIM IPv4 when multicast routing enabled
CSCsd38929	Yes	SSL: Verisign imported certificate fails when establishing SSL session
CSCsd39029	Yes	Traceback with Thread Name: Dispatch Unit
CSCsd40729	Yes	WebVPN page doesn't complete load and will hang browser
CSCsd40812	Yes	Internal WebVPN Page will not display after login
CSCsd42895	Yes	LDAP Base(Search) DN scope not working correctly
CSCsd43093	Yes	Memory leak due to SNMP monitoring on L2L IPSec tunnel
CSCsd43105	Yes	Traceback in SNMP thread under low memory condition
CSCsd43770	Yes	LDAP server-type configuration is not processed correctly.
CSCsd43909	Yes	LDAP Authen against AD does not work with Userid
CSCsd43976	Yes	ASA should not send names in split-tunnel list to SVC
CSCsd45099	Yes	logging debug-trace should not prevent debugs from printing to console
CSCsd45297	Yes	Syslog 722020 needs to include Tunnel-group name or be re-worded
CSCsd46111	Yes	Traceback when using sh xlate via telnet over VPN tunnel
CSCsd46373	Yes	ASA: WebVPN NTLM login fails if domain is not specified
CSCsd46685	Yes	Traceback eip::snp_sp_action_construct_ip_key+1013 after ipsec rule cfg
CSCsd46922	Yes	High CPU usage when configuring/compiling ACL's



**Table 3** *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCsd47171	Yes	GTP: IMSI prefix filtering on 3 digit MNC's do not work
CSCsd47976	Yes	Traceback on nameif command on unused intf with 8000 static commands
CSCsd48368	Yes	WebVPN - Domino Web Access Help Function hangs browser
CSCsd48512	Yes	Duplicate ASP crypto table entry causes firewall to not encrypt traffic
CSCsd48634	Yes	LDAP password management fails when connected to a MS Active Directory
CSCsd51884	Yes	Restore debug icmp trace functionality - showing nat translation
CSCsd52578	Yes	Traceback in thread: snp_timer_thread
CSCsd53213	Yes	PIX shows xlates from global xx.xx.xx.xx to local 0.0.0.0
CSCsd53232	Yes	Entire CIFS share not displayed when it contains more than 400 folders
CSCsd53321	Yes	sysopt connection timewait causes SSH sessions to timeout prematurely
CSCsd54293	Yes	ARP fails when PC moved from outside to inside of transparent FW
CSCsd55138	Yes	WebVPN: Traceback when accessing URL with Viewstate > 20K
CSCsd55527	Yes	traceback after executing sh cry ipsec sa sum with vpn sys test run
CSCsd58400	Yes	PIX fails to send Embryonic Limit Exceeded message
CSCsd58677	Yes	LDAP authentication succeeds if password is left blank
CSCsd58848	Yes	Memory allocated for connections not freed
CSCsd59936	Yes	Registering to the RP for PIM fails if fragmented in more then 12 packs
CSCsd63673	Yes	ASA with dhcprelay doesnt reply with unicast DHCP offer
CSCsd63828	Yes	PIX Failover does not Sync with certain multicast commands
CSCsd63863	Yes	CIFS Shares on Root Directory not displayed in alphabetical order
CSCsd64268	Yes	Secondary smtp-server fails to send event messages after period of time
CSCsd64584	Yes	http traffic fails with firewall in tfw and IPS monitoring in inline mod
CSCsd64912	Yes	url-server: tcp connections fail when tcp stack users are exhausted
CSCsd64920	Yes	url-server: url lookup requests are not retried when using tcp
CSCsd65192	Yes	WebVPN: Debug webvpn svc will not show up in show debug command
CSCsd65209	Yes	url-block block: http response buffering feature does not work
CSCsd65215	Yes	Capture access-list shows only 1 hit count for outbound traffic
CSCsd67028	Yes	WebVPN/SVC should disconnect if ASA encounters SSL CRYPTO Errors
CSCsd67905	Yes	HA Errors referencing WebVPN/VPN appearing even in Transparent mode
CSCsd68051	Yes	WebVPN: ActiveX component does not install when accessing MS TS URL
CSCsd69786	Yes	WebVPN: Duplicate/Malformed HTML Headers not transformed by ASA
CSCsd70242	Yes	Some syslogs are incorrectly logged to an event list, when not specified
CSCsd70812	Yes	HA: Traffic Stall after config syncing running Act/Act fover
CSCsd71386	Yes	RTSP traffic led the PIX to reload
CSCsd72617	Yes	Dispatch Unit Crash when HTTP inspect enabled...PIX/ASA 7.1.2, 7.0.4-11

**Table 3** *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCsd73035	Yes	URL's with + get re-written with space %20
CSCsd73060	Yes	Traceback in Dispatch Unit - on SVC connect (svc dpd-interval gateway)
CSCsd73376	Yes	Case-sensitive processing of javascript attribute
CSCsd73852	Yes	H.323 Inspect not opening media stream.
CSCsd74328	Yes	crash when changing security level on an ifc and failover cfg with NAT
CSCsd74964	Yes	SNP Inspect Http drops messages other than GET
CSCsd76384	Yes	dhcpd fails when management-access is configured
CSCsd77018	Yes	Traceback: Thread Name: Dispatch Unit (Old pc 0x00220087 ebp 0x01796d30)
CSCsd77155	Yes	All out of order packets dropped when queue-limit specified
CSCsd78595	Yes	Global buffer drop output under show service-policy
CSCsd79775	Yes	ASA VPN: all packets for a l2l peer get dropped instead of encrypted
CSCsd81288	Yes	UCTE functions not defined inside frames
CSCsd81668	Yes	Redirect for proxy-bypass links with high ports
CSCsd81969	Yes	LB configuration will be deleted when name is used in cluster ip add cmd
CSCsd82047	Yes	PIX 7.0(4) FO : bad LU from Act causes LU allocate xlate failed on Std
CSCsd82114	Yes	Change of log options on the ACE doesn't take immediate effect
CSCsd82355	Yes	Malformed syslog packets may be generated.
CSCsd83000	Yes	Invalid IPsec tunnel count is reported in ASDM handler output
CSCsd83007	Yes	Need ability to disable dns guard in 7.0
CSCsd83299	Yes	ASDM handler returns invalid value for ISAKMP SA's
CSCsd83863	Yes	Reload with Thread Name: Dispatch Unit
CSCsd84826	Yes	PIX/ASA MSS miscalculation for webvpn conn. terminating to the box
CSCsd85007	Yes	Dispatch unit traceback at snp_fp_fragment with SSM card enabled
CSCsd85345	Yes	Traceback may occur in fover_parse on 7.0.4
CSCsd86550	Yes	Traceback in snp_ids:ids_put when SSM is down
CSCsd89983	Yes	Access-list entered at line 1 is ineffective until access-group is rede
CSCsd91587	Yes	functioning email proxy session generates syslog message error
CSCsd92296	Yes	DHCP relay failed after failover
CSCsd93207	Yes	Show failover indicates different uptimes on devices in failover pair
CSCsd94089	Yes	Feature Req: Srcing auth pkts from inside(NEM)/assigned(CM) for IUA
CSCsd94386	Yes	Beta Customer Crash in inspect http
CSCsd94835	Yes	Proxy may queue too many packets when url filtering client is down
CSCsd94875	Yes	Traceback in VPN/IPsec CLI code when clear crypto ipsec sa counter
CSCsd95170	Yes	PIX 7.0(4)10 : reporting incorrect context CPU usage
CSCsd95480	Yes	Treatment of domain in JavaScript

**Table 3**     *Resolved Caveats (continued)*

ID Number	Software Version 7.2(1)	
	Corrected	Caveat Title
CSCsd97077	Yes	ASA/PIX - crash from SiVus SIP tester inside to outside w/ inspect/fixup
CSCsd97134	Yes	PIX/ASA ignores OSPF DBDs during adjacency building
CSCsd98071	Yes	conns fail after two successful authentications to virtual telnet IP
CSCsd98435	Yes	DHCPD pool does not allow to set ip add on interface once it is removed
CSCsd99200	Yes	Traceback in 7.1.2 caused by strict http inspection
CSCsd99326	Yes	Show service-policy crashes after global_policy change and interface add
CSCsd99709	Yes	PIX gets high cpu when type q to interrupt output of show conf
CSCse00303	Yes	Traceback during active/active config replication with 4 syslog servers
CSCse00756	Yes	URL filtering using Websense locks up downloads.
CSCse02703	Yes	Passwords in startup config may be changed without user intervention
CSCse02722	Yes	SSL Handshake failure with self signed cert
CSCse03299	Yes	VPN clients behind same PAT device using IPSEC/TCP & NAT-T fails IKE neg
CSCse05089	Yes	ASA 7.1(2) - Crash at listen/https w/ eip strdup:int3+4
CSCse05955	Yes	Java Applet with Cache_Archive PARAM Fail if No ARCHIVE Attribute
CSCse06536	Yes	ASA 7.1 : ASR not forwarding fragmented IP packets between contexts
CSCse08746	Yes	ASA send Radius attribute 31 source IP address as 0.0.0.0
CSCse10714	Yes	Shun behavior change in 7.x
CSCse11384	Yes	ASA crash in dhcp_daemon
CSCse14251	Yes	PIX with 7.1.2.4 crashes inside ntomain_process_ntinfo (ntomain.c)
CSCse19020	Yes	PPTP Pass-through not working due to inspection
CSCse20501	Yes	Passive FTP to Multinet server fails
CSCse22853	Yes	Active unit crash in accept/http when disabling DHCP relay
CSCse23164	Yes	PIX crash
CSCse23554	Yes	Memory leak within event_smtpmgr:es_SmtpSndMSG function
CSCse30479	Yes	tcp tx may not complete under certain conditions with proxy

## Related Documentation

Use this document in conjunction with the PIX Firewall and Cisco VPN client Version 3.x documentation at the following websites:

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/secursw/ps2308/tsd_products_support_series_home.html)

## Software Configuration Tips on the Cisco TAC Home Page

The Cisco Technical Assistance Center has many helpful pages. If you have a CDC account you can visit the following websites for assistance:

TAC Troubleshooting, Sample Configurations, Hardware Info, Software Installations and more:

<http://www.cisco.com/en/US/support/index.html>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

This document is to be used in conjunction with the documents listed in “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

© 2006 Cisco Systems, Inc.  
All rights reserved.